Remarks/Arguments

Claims 1, 3, 4, 6-13, 15-26 have been rejected. Claims 1, 11, 20, 24 and 25 have been amended to more distinctly point out and claim the subject matter the Applicant regards as their invention. Thus, claims 1, 3, 4, 6-13, and 15-26 are currently pending in the Application. Reconsideration of the application based on the claims as amended and arguments submitted below is requested. For all the reasons set forth herein, it is respectfully submitted that claims 1, 3, 4, 6-13, and 15-26 are now in condition for allowance.

Objections to the Drawings

input communication means including software for receiving a request for an authentication signal from a remote terminal

The Office Action objected to the drawings for failing to show "input communication means including software for receiving a request for an authentication signal from a remote terminal". However, FIG. 1 shows a number of input means 20, 22, 24, 26 and 32 all coupled to a processor 4 and a secure memory 40 that stores application software for the device. The functioning of the software with respect to the input devices is described in the first two paragraphs of the detailed description which describe the schematic of FIG. 1. The receiving of the request for the authentication signal by the input means and the processing of the received data is also described in the first paragraph of the Summary of the Invention.

9

wherein said device performs an initial verification of a user's identity prior to transmitting any data to an external device

The Office Action objected to the drawings for failing to show a method "wherein said device performs an initial verification of a user's identity prior to transmitting any data to an external device". Claim 24 has been amended to recite that the initial verification is performed prior to transmitting any "authentication data" to an external device to distinguish the transmission of data to the authentication server from the transmission of authentication data to an external device for initiation of a transaction. The device contacts the authentication server, as shown in steps 70 in FIG. 2 and 120 in FIG. 3 prior to performing an initial verification. However, this contact is only for the purpose of performing an audit check and updating the authentication server. Since this does not involve the transmission of any authentication data, the data is not susceptible to interception. However, it is respectfully submitted that FIGS. 2, 3 and 4 all show embodiments of the present invention "wherein said device performs an initial verification of a user's identity prior to transmitting any authentication data to an external device".

In particular, steps 60 through 90 of FIG. 2 illustrate the device verifying the user's identity prior to transmitting any authentication data to an external device in steps 92, 94 and 98.

Steps 110 -134 of FIG. 3, which bears the title authentication flow, illustrate the device verifying the user in steps 110-134 before trying to establish contact with the network in step 138.

10

FIG. 4 shows that the transaction flow, which involves transmitting data to an external device, only begins with the completion of the authentication process as shown in step 150.

FIGS. 2-4 and the authentication and verification processes of the present invention are well discussed in the detailed description and they clearly show that the present invention as described does not transmit any authentication data to an external device prior to verifying the user's identity. Therefore, it is humbly submitted that the recited claim limitation is in fact illustrated in the drawings.

"hardware or software that detects attempts to access data stored on the device or access a restricted portion of the device and erases stored data based upon said detection"

The Office Action took the position that the claim limitation "tamper resistant hardware or software that detects attempts to access data stored on the device or access a restricted portion of the device and erases stored data based upon said detection" was not shown in the drawings. However, the processor 4 shown in FIG. 1 is the hardware that holds the software that detects attempts to access the secure memory 40, the restricted portion of the device, which is erased when a an attempt is detected. Paragraph 0015 of the specification states that "The memory 40 is secure in that, even when in standby mode or awaiting authentication by the user or other instructions received through one of the device's communications channels, a diagnostic and monitoring program runs to guard against attempts to

11

hack into the device's memory 40 either by physical penetration or logical probe. In the event security is compromised, the device is programmed to clear significant portions of the data stored in its memory 40 to render the device and data useless to an attacker". The described diagnostic check is also shown in FIG. 2, step 72, and FIG. 3, step 112. There is no requirement that every single word used in the claim or specification appear in the drawings. Nevertheless, Applicant has amended claim 25 to remove the term "tamper resistant" since the actual term does not appear in the specification However, Applicant respectfully submits that "tamper resistant" fairly describes the functioning of the device in erasing the secure memory 40 upon detecting an unexpected attempt to access the memory. The actual source code to implement this function will depend upon the processor and programming language used and is well within the skills of an average programmer. Applicant has a working model.

The specification also states with respect to FIG. 2 that "the method then proceeds to block 72 wherein a diagnostic check of the token's electronics systems is performed. If the diagnostic test is passed, the token is interrogated to determine if its biometric data storage is ready to be used in an identification process as shown in block 74. If the token fails either the diagnostic test or the biometric data check, the method proceeds to block 76 wherein a error message is displayed to a user of the token and the token is powered down.

12

"wherein an identity of the remote terminal is verified to ensure that the remote terminal is a known or authorized source"

The Office Action objected to the drawings for failing to show "wherein an identity of the remote terminal is verified to ensure that the remote terminal is a known or authorized source". In steps 154 and 172 of FIG. 4, the token is shown handshaking with a smart chip device and a server through personal key identified transaction. Personal key identified transactions are examples of the present invention's ability to verify the identity of a remote terminal to ensure that the remote terminal is a known or authorized source. A corresponding discussion of personal key identified transactions and the steps shown in FIG. 4 is set forth in the detailed description. Therefore, it is respectfully submitted that the drawings do show a method "wherein an identity of the remote terminal is verified to ensure that the remote terminal is a known or authorized source".

Specification Objections and Claim Rejections under 35 U.S.C. § 112

The Office Action objected to the Specification as failing satisfy the written description requirement under 35 U.S.C. § 112 and failure to provide antecedent basis for a number of the claim limitations. The basis for these rejections mirrored the Office Actions objections to the drawings.

input communication means including software for receiving a request for an authentication signal from a remote terminal

In particular, the Office Action objected to the Specification as failing to satisfy the written description requirement and provide antecedent basis for the claim limitation "input communication means including software for receiving a request for an authentication signal from a remote terminal".

The receiving of the data by the input means and the processing of the received data are described verbatim in the first paragraph of the Summary of the Invention. The first embodiment disclosed is explicitly described as a hand held device wherein "Input communication means receive a request for an authentication signal from a remote terminal. In response to the received request for an authentication signal or a manual activation by a user, a biometric sensor detects biometric information and produces a sensed biometric profile. A biometric profile corresponding to an individual is contained in a memory on the hand-held device. The memory also contains certification information that can be examined by a remote terminal to determine if the device corresponds to an authorized account. The processor compares the sensed biometric profile with the stored biometric profile and produces an authentication signal." Therefore, it is respectfully submitted that the recited input means clearly has antecedent basis in the specification.

Paragraph 0018 of the specification further states "the device may perform a number of authorization functions such as producing and communicating authentication signals". As stated with respect to the drawing objections FIG. 1 shows a number of input means 20, 22, 24, 26 and 32 all coupled to a processor 4

14

and a secure memory 40 that stores the software for the device that allows the device to receive the authentication signal. The specification states that "The secure memory 40 includes ROM memory that contains static information needed to operate the device and RAM that can store application software that can be run on the device."

Applicant respectfully contends that the recited input communications means is described in great detail in the specification in such a way as to convey to one skilled in the art that Applicant had possession of the claimed invention. Provided the motivation of the present application, preparing software for a particular processor that will "receive a request for an authentication signal from a remote terminal" is well within the skills of an average programmer. Applicant has had a working model of the invention since the filing of the application.

As a further example, the Specification describes how "The speaker 14 and microphone 10 are used in conjunction with voice recognition software to receive voice commands from a user, communicate audible messages to the user and perform biometric identification processes." The speaker 14 and microphone 10 are input communication means and the included voice recognition software is used to receive their output and authenticate the speaking individual in response to a request.

"wherein said device performs an initial verification of a user's identity prior to transmitting any data to an external device"

The Office Action objected to the Specification as failing to satisfy the written description requirement and provide antecedent basis for the claim limitation "wherein said device performs an initial verification of a user's identity prior to transmitting any authentication data to an external device". However, as discussed with respect the objections to the drawings, FIGS. 2, 3 and 4 all show embodiments "wherein said device performs an initial verification of a user's identity prior to transmitting any authentication data to an external device". Steps 60 through 90 of FIG. 2 illustrate the device verifying the user's identity prior to transmitting any authentication data to an external device in steps 92, 94 and 98. Steps 110 -134 of FIG. 3, which bears the title authentication flow, illustrate the device verifying the user in steps 110-134 before trying to establish contact with the network in step 138. FIG. 4 illustrates the transaction flow which only begins with the completion of the authentication process as shown in step 150. Every step of these figures is discussed in detail in the specification in the sections corresponding to the figures.

"hardware or software that detects attempts to access data stored on the device or access a restricted portion of the device and erases stored data based upon said detection"

The Office Action took the position that the claim language "tamper resistant hardware or software that detects attempts to access data stored on the device or access a restricted portion of the device and erases stored data based upon said

16

detection" was not enabled by the specification or provided with antecedent basis. However, paragraph 0015 of the specification states that "The memory 40 is secure in that, even when in standby mode or awaiting authentication by the user or other instructions received through one of the device's communications channels, a diagnostic and monitoring program runs to guard against attempts to hack into the device's memory 40 either by physical penetration or logical probe. In the event security is compromised, the device is programmed to clear significant portions of the data stored in its memory 40 to render the device and data useless to an attacker".

The specification also states with respect to FIG. 2 that "the method then proceeds to block 72 wherein a diagnostic check of the token's electronics systems is performed. If the diagnostic test is passed, the token is interrogated to determine if its biometric data storage is ready to be used in an identification process as shown in block 74. If the token fails either the diagnostic test or the biometric data check, the method proceeds to block 76 wherein an error message is displayed to a user of the token and the token is powered down.

Although the specification clearly describes "tamper resistant" software and hardware, Applicant has deleted the term "tamper resistant" since that exact language is not in the specification. Applicant respectfully asserts that the claim language "hardware or software that detects attempts to access data stored on the device or access a restricted portion of the device and erases stored data based upon said detection" is taken almost directly from the specification of the patent and,

provided the motivation of the present application, software that performs a diagnostic check and erases data in the event of a failure is well within the skill of an average programmer.

Claim Rejections - 35 U.S.C. § 103(a)

Claim 1 was rejected under 35 U.S.C. § 103(a) as being unpatentable over Maes et al (U.S. Patent No. 6,016,476) in view of U.S. Patent Publication 2003/0149662 A1 to Shore. For all the reasons set forth herein, it is respectfully requested that the rejection of Claim 1 under 35 U.S.C. § 103(a) should be withdrawn.

Claims 1 recites a portable device having "a magnetic strip permanently attached to the portable device that is readable by a standard swipe card reader" and "a biometric sensor for detecting biometric information and producing a sensed biometric profile in a response to a received request for an authentication signal". Maes does not disclose a device with a magnetic strip permanently attached to the device. Rather, Maes configures a card 26 having a magnetic stripe for use as a selected credit card with a PDA 10. The card 26 does not have a biometric sensor and the PDA 10 does not have a readable magnetic strip that can interface with a card reader. Thus, neither the card 26 nor the PDA 10 of Maes has both a biometric sensor and a readable magnetic strip. Conversely, claim 1 recites a magnetic card swipe interface permanently attached to a portable device with a biometric sensor. The present invention as recited in claim 1 eliminates the step of configuring the

18

card with the device and then using the card to interface to the card reader and, thus, is an improvement upon Maes. Shore also does not disclose a device having a biometric sensor with a readable magnetic strip on the device itself.

Regarding claim 3, none of the output communication means disclosed in Maes or Shore are proximity antennas. Such an antenna provides a distinct advantage over the references because it allows the device to be used by simply placing the device in proximity to the reader while not outputting easily interceptable transmissions that are detectable from a long distance. There is also no suggestion in either reference that they would benefit from the use of such an antenna.

Claim 5 is dependent upon claim 1 and therefore allowable for all the reasons stated above with respect to claim 1.

Claim 6 is dependent upon claim 1 and, therefore, allowable for all the reasons stated above with respect to claim 1.

With regard to claim 7, neither Maes nor Shore discloses a device that has a processor that can manipulate information on a magnetic strip permanently attached to the portable device. A smart card such as disclosed in Maes uses electrical contacts 30, not a magnetic stripe, on the card to connect with a terminal. The present invention as recited in claim 7 is beneficial in that the portable device itself can interface with a magnetic stripe reader in an alterable manner.

Claims 8 and 9 are dependent upon claim 1 and, therefore, allowable for all the reasons stated above with respect to claim 1.

With regard to claim 10, the universal card 26 is not the PDA 10 in Maes and the PDA 10 in Maes does not have a protrusion that is adapted to engage a swipe card reader. Rather, Maes uses the removable card 26 to interface with a card reader. The present invention as recited in claim 10 is an electronic device with a processor that has the recited communication means and power supply and "a protrusion that is adapted to engage a swipe card reader". A clearly different device than that disclosed or suggested in either Maes or Shore.

Regarding claim 11, claim 11 recites an electronic data assistant that has "a card swipe interface **permanently attached to the electronic data assistant** that allows stored data to be communicated to a magnetic card reader" and "a processor for comparing said personal identification information and producing an authentication signal based upon said comparison". Maes does not disclose an electronic data assistant that has "a card swipe interface permanently attached to the electronic data assistant". Rather, the device of Mayes transfers data to a card reader 30 by configuring a card 26 with a PDA 10 and then uses the card 26 to interface with the card reader 30. The present invention as recited in claim 11 eliminates the step of configuring the card with the device and then using the card to interface to the card reader and, thus, is an improvement upon Maes and not disclosed or suggested in Shore.

Claims 12, 13 and15 are dependent upon claim 11 and, therefore, allowable for all the reasons stated above with respect to claim 11.

20

Claim 16 recites an electronic data assistant having a proximity antenna that is not disclosed in either Maes or Shore.

Claims 17 and 18 are dependent upon claim 11 and, therefore, allowable for all the reasons stated above with respect to claim 11.

Claim 19 recites the electronic data assistant of claim 11 wherein "the card swipe interface further comprises a blade-shaped protrusion adapted to be accepted by a card reader". This feature is totally lacking in any of the devices disclosed in the cited references.

Claims 20-23 were rejected under 35 USC 103(a) as being unpatentable over U.S. Patent No. 5,917,913 to Wang in view of Maes.
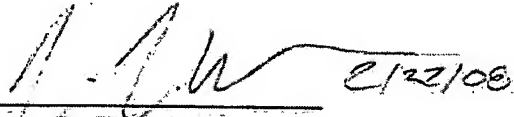
Claim 20 has been amended to more distinctly point out that "the portable electronic device has **a magnetic strip permanently attached to the portable device that is readable by a standard swipe card reader"**. None of the cited references discloses a portable electronic device with a magnetic strip constructed on the device itself.

Claims 21-23 are dependent upon claim 20 and therefore allowable for all the reasons stated above with respect to claim 20.

Claims 24-26 depend from claim 1 and therefore are allowable for the reasons stated above with respect to claim 1. Neither the Anderson reference nor the Schneider reference discloses a device having a permanently attached magnetic strip.

21

For all the reasons stated herein it is respectfully submitted that the application is now in condition for allowance.

Respectfully submitted,

Jason L. Hornkohl   2/22/08

Jason L. Hornkohl
Registration No. 44,777
Hornkohl Law Firm

ATTORNEY FOR APPLICANT

Jason L. Hornkohl
Hornkohl Law Firm
P.O. Box 210584
Nashville, TN 37221
(615) 673-6771